CONFIGURATION MIGRATION UTILITY

FortiConverter™ 4.5

User Guide

FortiConverter™ 4.5 User Guide

October 14, 2014

Revision 1

Technical Documentation	docs.fortinet.com
Knowledge Base	kb.fortinet.com
Customer Service & Support	fconvert_feedback@fortinet.com
Training Services	training.fortinet.com
FortiGuard	fortiguard.com
Document Feedback	techdocs@fortinet.com

Table of contents

Introduction

This document shows how to install and use FortiConverter.

FortiConverter is designed to help you migrate your network to Fortinet network security solutions, significantly reducing workload and minimizing errors. FortiConverter translates configuration files from other vendors' firewall products into a valid FortiGate or FortiManager configuration file. Because the output uses command line syntax, it can either be uploaded as a configuration file or piped to the CLI.

For additional assistance, please contact fconvert_feedback@fortinet.com.

Supported vendors & configuration objects

FortiConverter can translate configurations from the following vendors and platforms.

In some cases, FortiConverter cannot translate some parts of the configuration because of dependencies or unsupported syntax and you must manually convert them.

If the number of objects exceeds the maximum valid length for FortiGate or FortiManager, FortiConverter trims them.

Vendor	Models	Versions	Convertible objects
Alcatel-Lucent	Brick	v9.x	Addresses & Address Books Interfaces (physical, logical, loop-back, PPPoE) Partitions Services & Service Books Static routes Zone rule set
Check Point	SmartCenter Provider-1	NG FP1 (4.) to NGX R64/R71/R75/R76	Addresses & Address Groups Interfaces (Physical, Logical, Loop-back, PPPoE) Local Users & Groups NAT (Automatic & Rule) Negate Cell Policies (rulebases.fws) RADIUS, TACACS+, & LDAP Rules Schedules Services & Service Groups Static routes VPN (IPSec)

Vendor	Models	Versions	Convertible objects
Cisco	PIX ASA FWSM	4.x to 8.x	ACLs Addresses & Address Groups DHCP Servers DNS Servers Interfaces (Physical, Logical, Loop-back, PPPoE, Tunnel) IP Pools Local Users & Groups NAT (including Object NAT and Double NAT) RADIUS, TACACS+, & LDAP Services & Service Groups Static Routes Time Ranges VPN (IPSec, PPTP/L2TP, EZVPN)
	IOS	10.x to 12.x 15.x	
Juniper	SSG	ScreenOS/JunOS 5.x to 6.x	Addresses & Address Groups & FQDNs DHCP Servers & Clients & Relays Interfaces (Physical, Logical, Loop-back, PPPoE, Tunnel) Static Routes Services & Service Groups Policies VIPs/MIPs NAT IP Pools VPN (IPSec, PPTP/L2TP) Local Users & Groups RADIUS & LDAP Zones
	SRX	JunOS 10.x, 11.x, 12.x	Addresses & Address Groups & FQDNs DHCP Servers & Client & Relay Interfaces (Physical, Logical, Loop-back, PPPoE, Tunnel) IP Pools Local Users & Groups NAT Policies RADIUS & LDAP Services & Service Groups Static Routes VIPs/MIPs VPN (IPSec, PPTP/L2TP) Zones

Vendor	Models	Versions	Convertible objects
Palo Alto Networks	PA	PAN-OS 1.x to 6.x	Addresses & Address Groups & FQDNs Interfaces Local Users & Groups NAT (partial) Policies Schedules Static Routes Services & Service Groups Zones
SonicWall	NSA Serials	SonicOS Enhanced 5.x	Addresses & Address Groups & FQDNs DHCP Servers & Clients & Relays Interfaces (Physical, Logical, Loop-back, PPPoE) Local Users & Groups NAT Policies Schedules Services & Service Groups Static Routes Zones

Licensing

The free-license FortiConverter software has the following limitations:

- No fine-tuning feature, which allows you to manually adjust migration settings and review the result of your changes before you generate an output file.
- Conversion output is limited to 100 lines of CLI configuration. You can view the full conversion, but the software saves only 100 lines in the output configuration file.
- SonicWall conversion is not supported

After you purchase and upload a license, FortiConverter is unlocked and these limitations are removed. Your paid license entitles you to any new versions of FortiConverter that Fortinet releases until the license expires.

For more information, see "Uploading the license" on page 11

System requirements

FortiConverter requires one of the following operating systems:

- Microsoft Windows 8 (32-bit or 64-bit)
- Microsoft Windows 7 (32-bit or 64-bit)
- Microsoft Windows Vista (32-bit or 64-bit)
- Microsoft Windows XP (32-bit)

In addition, FortiConverter requires .NET Framework 4.0. If it is not already installed on your computer, the FortiConverter installer prompts you to download and install it.

A web browser is required to view conversion reports.

What's new

The following list contains features that are new or enhanced for FortiConverter™ 4.5.

- **Palo Alto Networks firewall conversion** – FortiConverter can now convert a Palo Alto Networks firewall configuration to a FortiOS configuration. See "Supported vendors & configuration objects" on page 5.
- **Batch mode for retail branch conversion** – You can now convert a group of firewalls using a single operation. See "Using retail branch batch conversion mode" on page 27.
- **Automatically check for updates** – You can configure FortiConverter to automatically check for software updates. See "Updating the software" on page 13.
- **Configurable policy index values** – You can now select the initial policy number that FortiConverter uses in a converted configuration. See "Fine-tuning" on page 33.
- **Output file directory** – FortiConverter now saves converted configurations as files in a directory with the name of the input file. If subsequent input files have a different name, it preserves any previous output files.

Installation

Installing the software

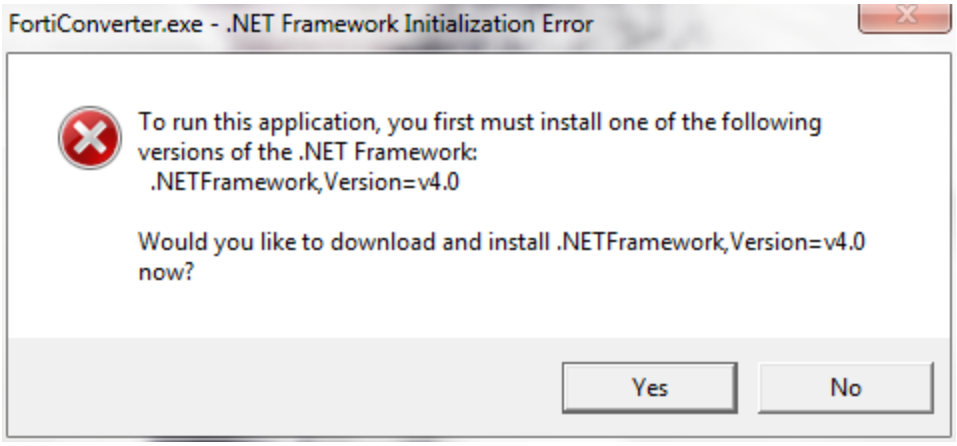
To download the FortiConverter installer from the Fortinet Technical Support web site, go to:

https://support.fortinet.com

To install FortiConverter

1. Double-click the FortiConverter installer executable (.exe).

   If your computer does not have Microsoft .NET Framework 4.0, you are prompted to install it.



2. To proceed with the installation, click **Yes** and then download the software framework from Microsoft's web site.
3. To continue the installation, read the license agreement, select **I accept the terms of the License Agreement**, and then click **Next**.
4. If you want to install the program in a location that is different from the default one, click **Browse** and select the directory.
5. Click **Next**.
6. Select the Start Menu folder that you want to add the program shortcuts to, and then click **Install**.
7. Click **Finish** to exit the FortiConverter installer.

Uploading the license

By default, FortiConverter is installed with a limited, free license. If you have purchased an full license, upload it to unlock the complete feature set.

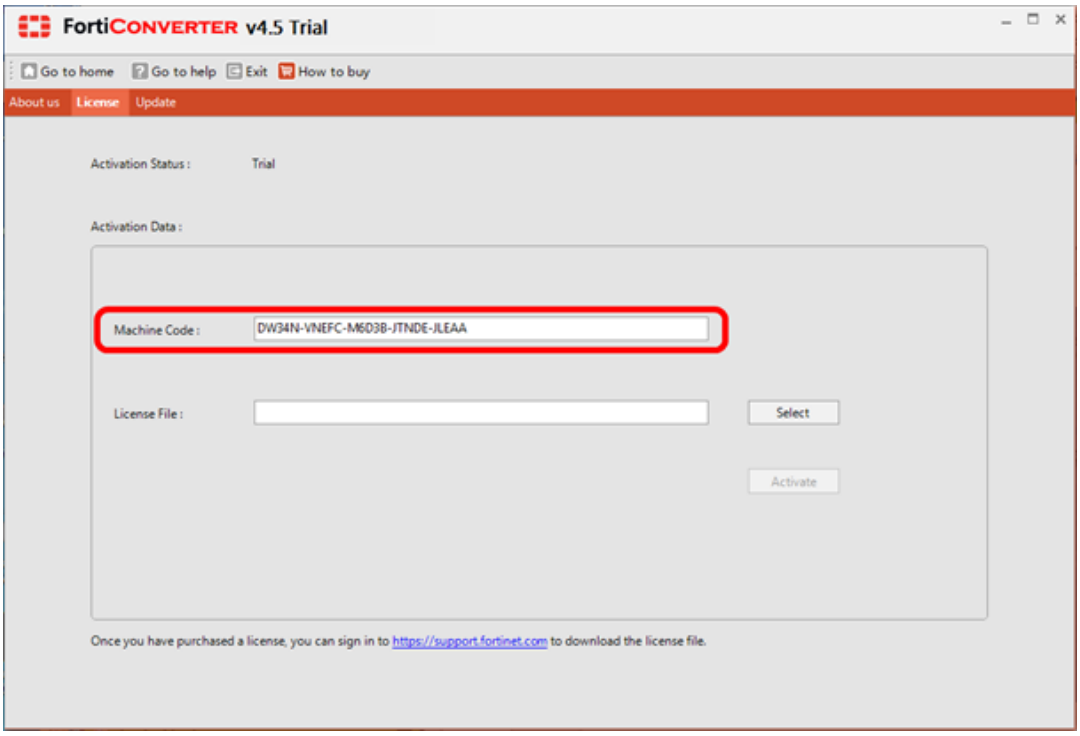
To activate the license

1. To start FortiConverter, double-click its shortcut.

2. Click **License Activation**.

If the license is already activated, the **License Activation** square is not displayed. To access License information, click **System Setting**, and then click the **License** tab.

3. Click the **License** tab.
4. Copy the **Machine Code** value to the clipboard.

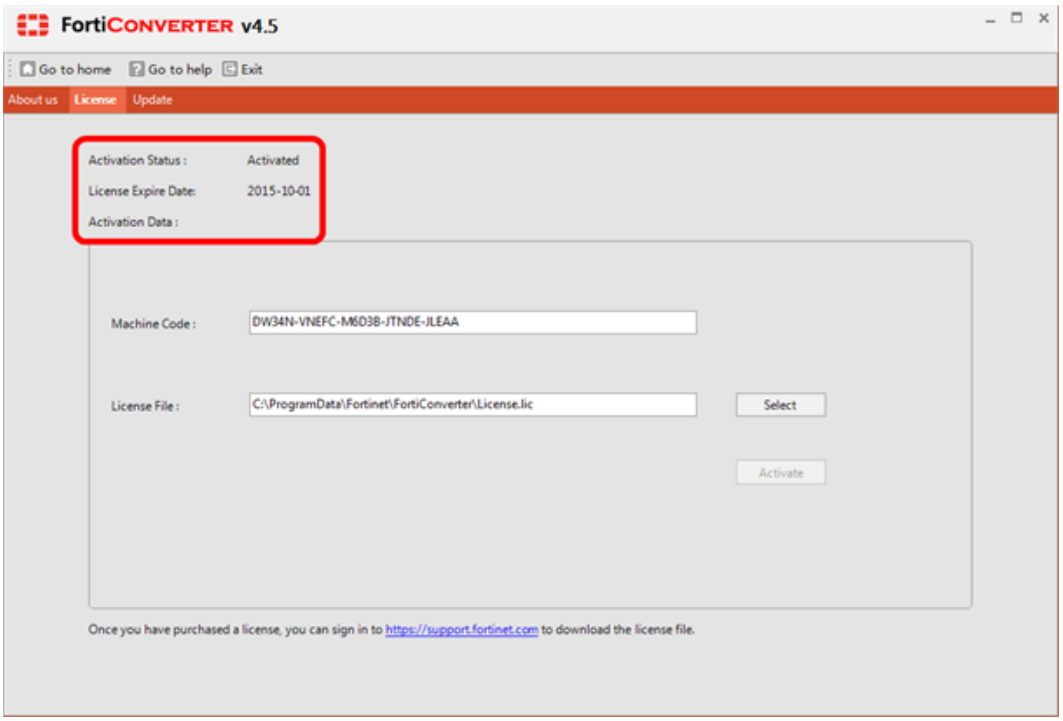


5. In a web browser, go to the Fortinet Technical Support web site:

   https://support.fortinet.com/

6. Enter your machine code to activate and download your FortiConverter license (.lic file).
7. In FortiConverter, on the License tab, click **Select** and navigate to the .lic file to select it.
8. Click **Activate**.

   FortiConverter validates the license file and changes the value of **Activation Status** from **Free** to **Activated**.



Your license is valid for all FortiConverter software updates released until the **Expire Date** value.

After the license is activated, to access the expiry information, on the home page, click **System Setting**, and then click the **License** tab.

Updating the software

Your FortiConverter license is valid for all software updates released until it expires.

You can check for and install software updates manually or configure FortiConverter to automatically check for updates each time you open the application for the first time that day.

To check for software updates

1. On the home page, click **System Setting**,
2. Optionally, to review the expiry date for your license, click the **License** tab.
3. Click the **Update** tab.
4. Optionally, to have FortiConverter automatically check for updates when you open the application for the first time that day, select **Auto check and update**.
5. To manually check for updated software, click **Go!**.

   FortiConverter displays a message that the software is up-to-date or that an update is

available.

6. If an update is available, confirm that you want to download it.

Conversion

FortiConverter provides wizards that convert configuration files from a specific vendor to FortiGate or FortiManager configuration files. After you input information about your previous vendor's configuration files, you can preview and fine-tune the conversion before you output the final FortiGate or FortiManager configuration file.

Downloading the source configuration files

Before you start the conversion wizard, download your existing configuration to the computer where FortiConverter is installed. Procedures vary by vendor.

Some vendors divide the configuration into multiple files, so make sure that you download all files.

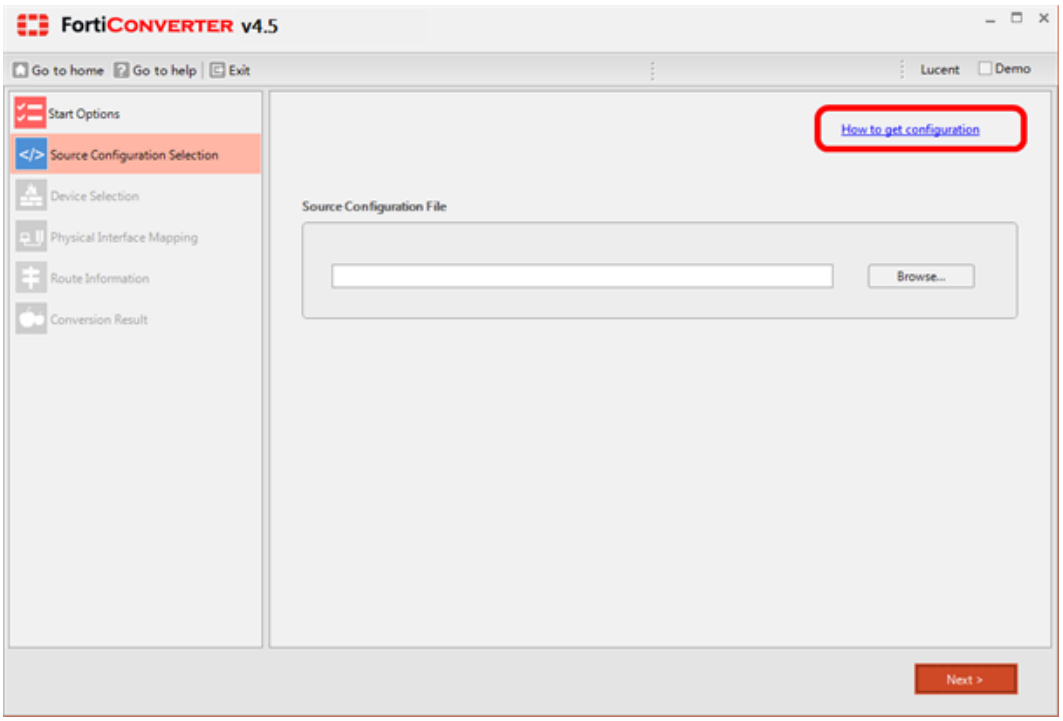
Alcatel-Lucent

FortiConverter provides a Perl script for downloading Alcatel-Lucent Brick configurations.

To access the Alcatel-Lucent configuration download script

1. On the FortiConverter home page, click the Alcatel-Lucent square.
2. On the Start Options page, click **Next**.

   If you are using the wizard to retrieve the download script only, use the default settings for this page. You can restart the wizard later after you have the file and are ready to perform the conversion with the appropriate settings.
3. On the Source Configuration Selection page, click **How to get configuration**.



The Windows folder that contains the Perl script and the documentation for using it are displayed. Follow the instructions to run the Perl script and output the source configuration as a set of directories.

Check Point

To acquire the configuration, download the following files:

- Object definitions – 'objects_5_0.c' (Check Point NG/NGX) or 'objects.c' (Check Point 4.x) contains the firewall's object definitions. To convert from Platform-1, 'mcss.c' contains the MDS hierarchy files.
- Policy and rule definitions – '*.w' or 'rulebases_5_0.fws'. The file name is <rule>.W (default Standard.W). or rulebases_5_0.fws. They are located in the directory "[SmartCenter]\fw1\conf\".
- Route information – Helps FortiConverter to correctly interpret the network topology being converted. To get this data, enter the `route print` command, then copy and paste the output into a plain text file. Codes in the output indicate if the route is a directly connected interface, a host route, a network route, and so on. The output varies by the platform.
- User and user groups file – fwauth.NDBx

Juniper

To obtain the configuration, use one of the following methods:

- In the web UI, go to **Configuration > Update > ConfigFile**.
- Using the CLI, paste the output of the `get conf` command into a plain text file.

Palo Alto Networks

In the web UI, go to **Device > Setup > Operations**, and then click **Export named configuration snapshot**.

SonicWall

To download the configuration (*.exp file), in the web UI, go to **System > Settings > Export Settings**.

Using the conversion wizard

FortiConverter guides you through the conversion process and automatically migrates as much of the source configuration as possible. After the initial conversion, you can review and fine-tune the results manually before you export the final FortiGate or FortiManager configuration file.

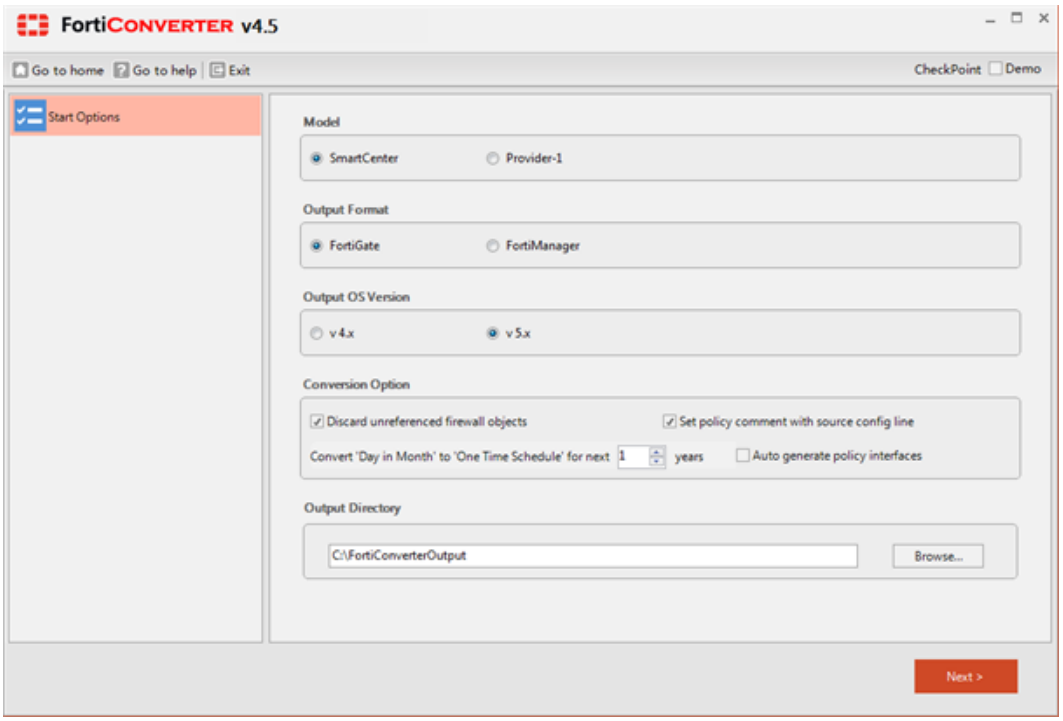
The following steps illustrate a conversion using a Check Point firewall, which in most cases is similar to converting firewalls from other vendors. However, to convert a Check Point Provider-1 configuration, see "Using the conversion wizard with Check Point Provider-1 files" on page 23.

After you have specified the source configuration, but before you navigate to the Conversion Result page, you can return to a previous step in the wizard by clicking its name in the panel on the left side.

You can also use the **Retail Branch Batch Mode** option the wizard to convert a group of similar source configurations in a single operation. The page where you select this option depends on the type of configuration. For more information, see "Using retail branch batch conversion mode" on page 27.

To migrate your configuration

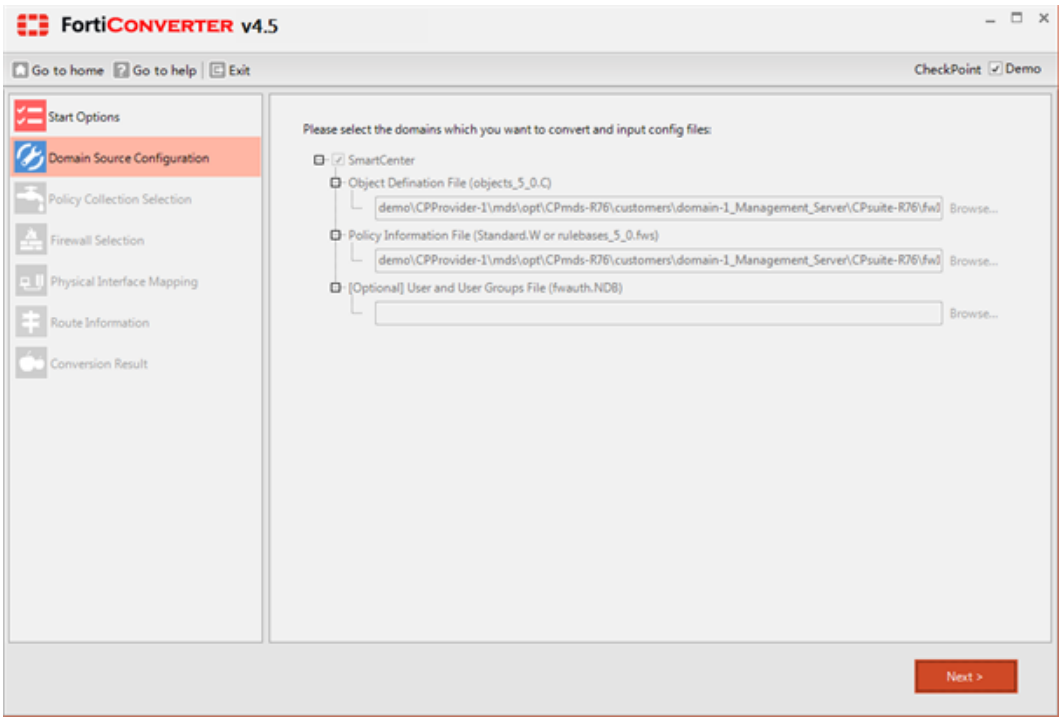
1. On the FortiConverter home page, click the square for the appropriate vendor.
2. In the **Start Options** page, complete the settings as required.



For example, specify your old firewall or centralized management model, whether the output is for FortiGate or FortiManager, whether or not to discard unreferenced objects and comments, and the directory where you want to save output files.

You can also define how to handle the “Day in Month” setting on Check Point firewalls. Check Point firewalls have a time object that specifies days of the month, which does not exist on FortiGate. By default, FortiConverter creates FortiGate one-time schedules for a year – one schedule per date. You can specify that FortiConverter creates more than one year of schedules, or select 0 to create no schedules. For more information, see the Check Point section in "Understanding your new configuration" on page 37.

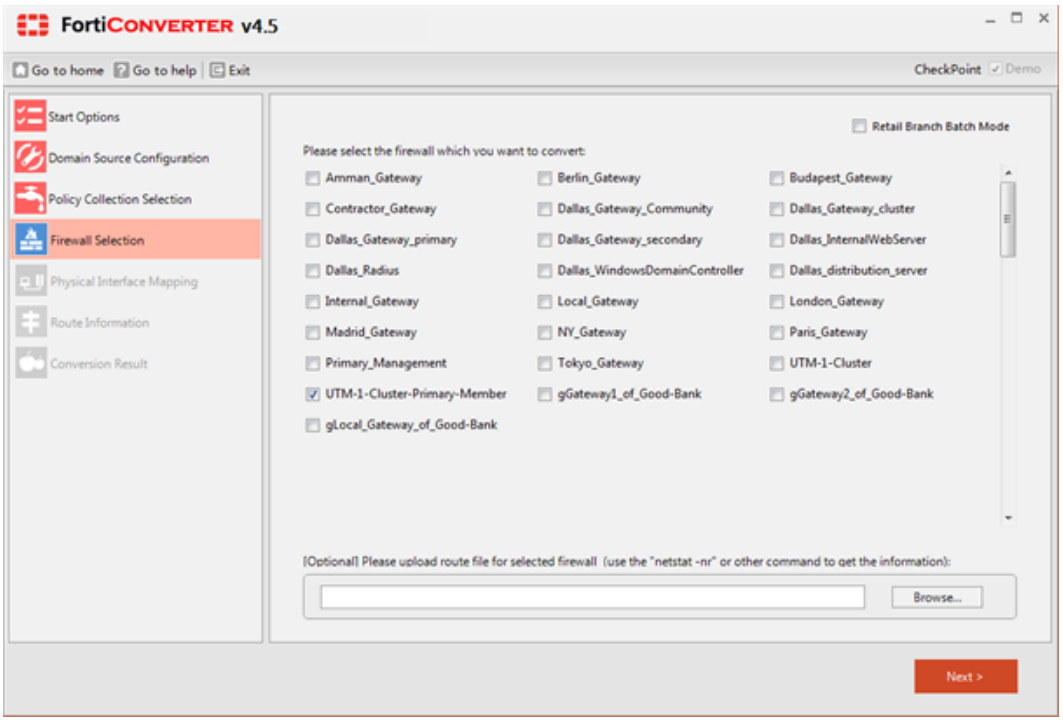
3. Click **Next**.
4. Browse to the configuration files that you obtained earlier to select them.



5. Click **Next**.
6. On the Policy Content Selection page, select one or more policy packages to convert, then click **Next**.
7. If you are migrating from Check Point, on the Firewall Selection page, select the appropriate model.

   Check Point can store multiple firewalls in the object definition file.

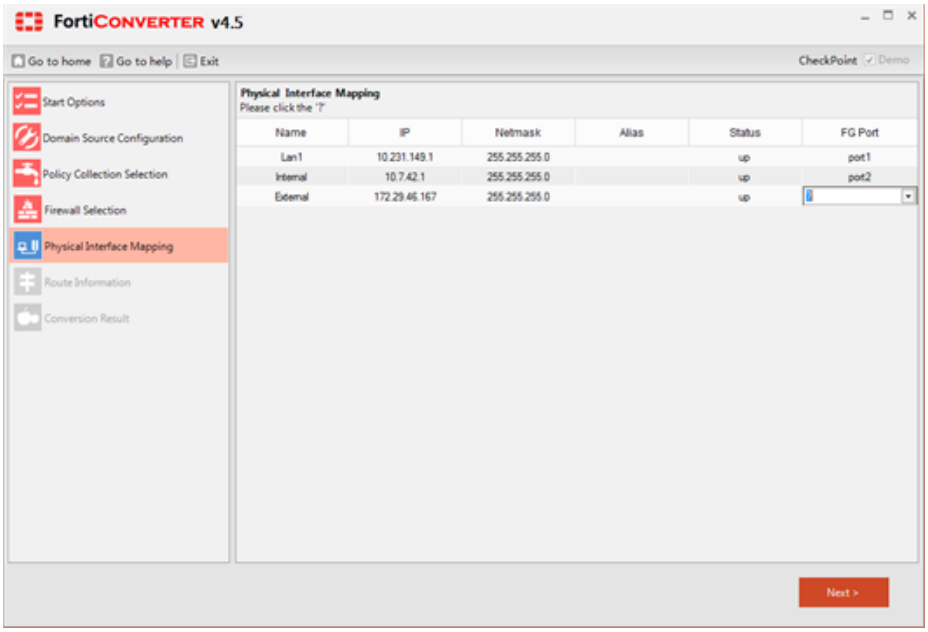
   If the configuration file that you downloaded contains only one model, you may not need to select anything.



For Check Point, if your source configuration files include a route information file, click **Browse** to navigate to the file and select it.

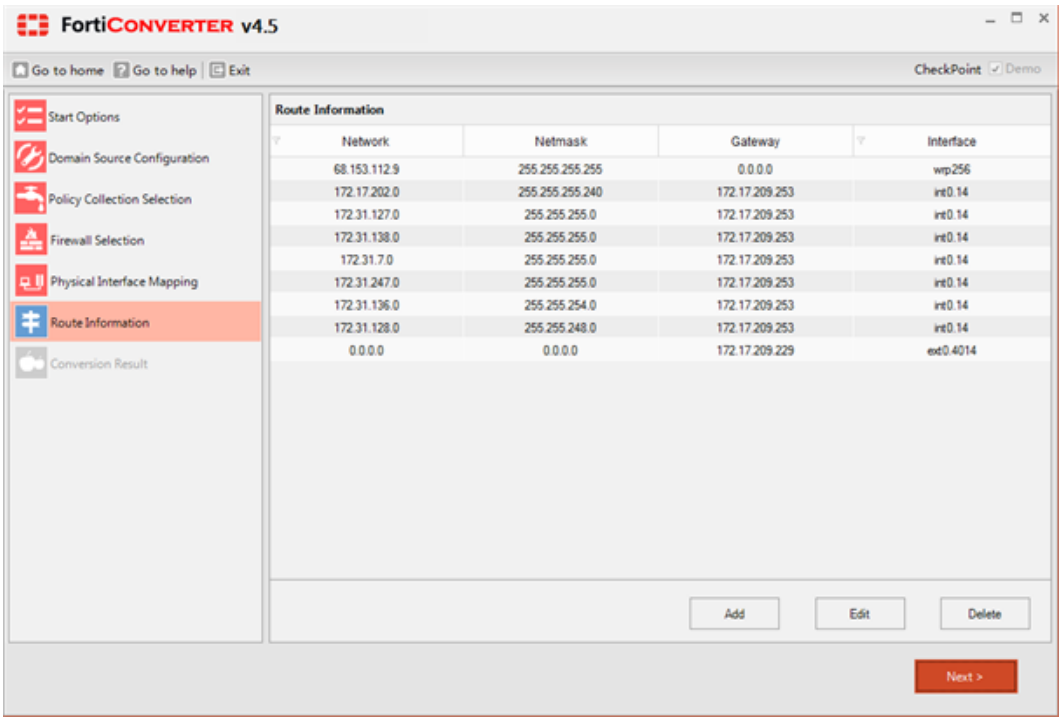
For more information on creating the route information file, see the Check Point information under "Downloading the source configuration files" on page 15.

8. Click **Next**.
9. Specify the new names for the Check Point, Cisco, Juniper, or SonicWall network interfaces on your FortiGate firewall.



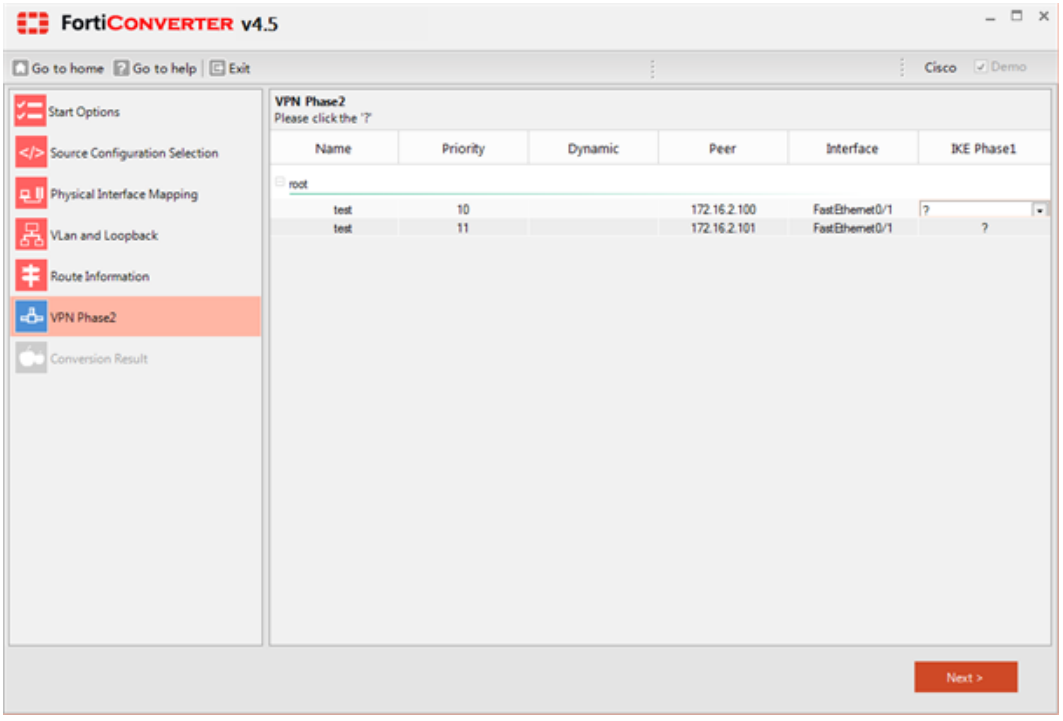
10. Click **Next**.
11. If there are logical interfaces such as VLANs or loopback interfaces defined in the configuration that you are converting, verify their conversion. To correctly interpret the direction of rules and interfaces, add routing information.

    FortiConverter does not include temporary routes in the final configuration.

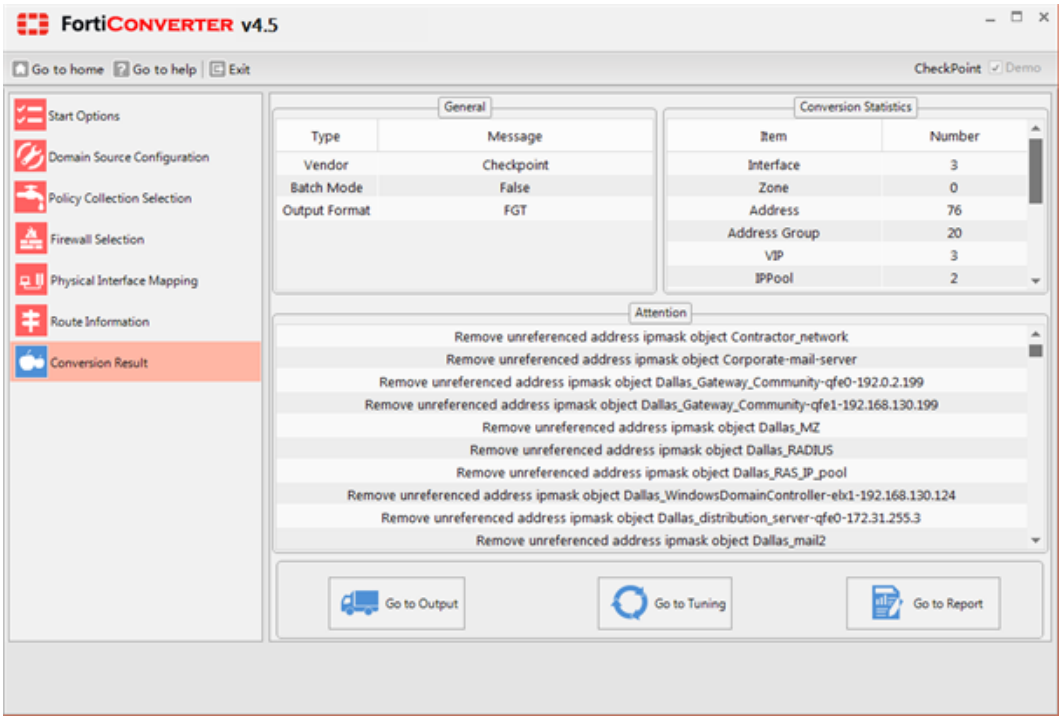


12. Click **Next**.

13. If you are converting Cisco IPSec Phase 1 and Phase 2 definitions, enter them manually. FortiConverter cannot convert them automatically.



14. Click **Next**.



15. Do one of the following:

- Click **Go to Report** to see a summary of the conversion, including objects that the wizard did not convert. For more information, see "Viewing the results of your automatic conversion" on page 32.
- Click **Go to Tuning** to adjust the converted settings before you generate the final output configuration. For more informatinon, see "Fine-tuning" on page 33.
- Click **Go to Output** to view the final converted configuration files.

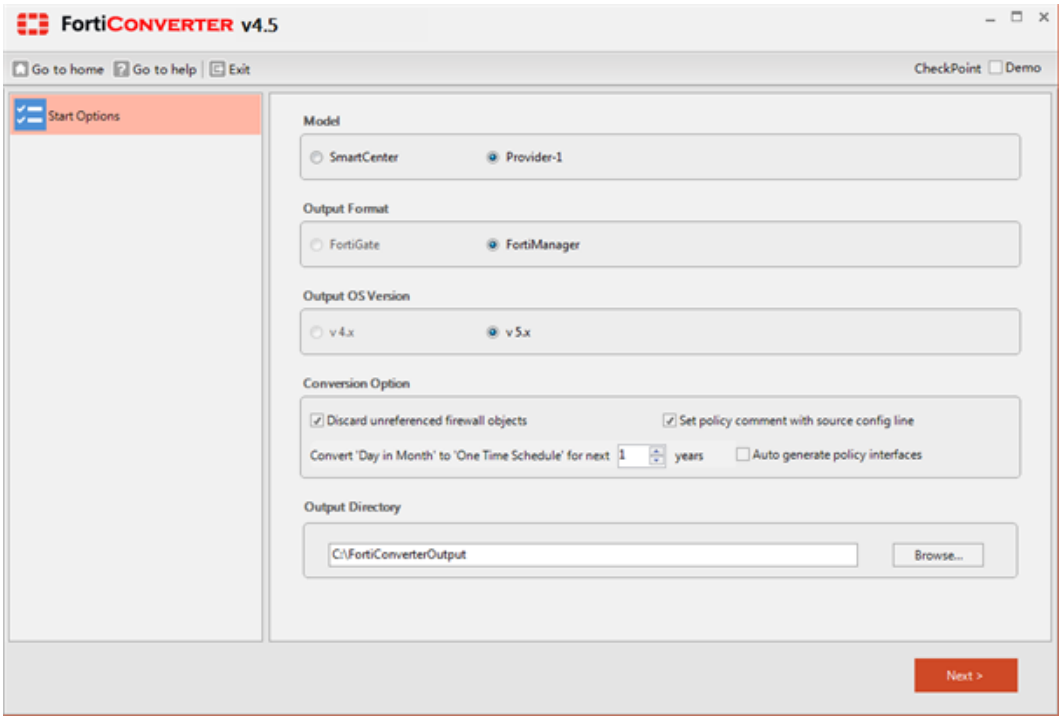
Using the conversion wizard with Check Point Provider-1 files

Conversion from a Check Point Provider-1 is different from other types of configuration conversions.

To migrate your configuration

1. In FortiConverter, click **Check Point to FortiGate**.
2. In the **Start Options** page, complete the settings as required.

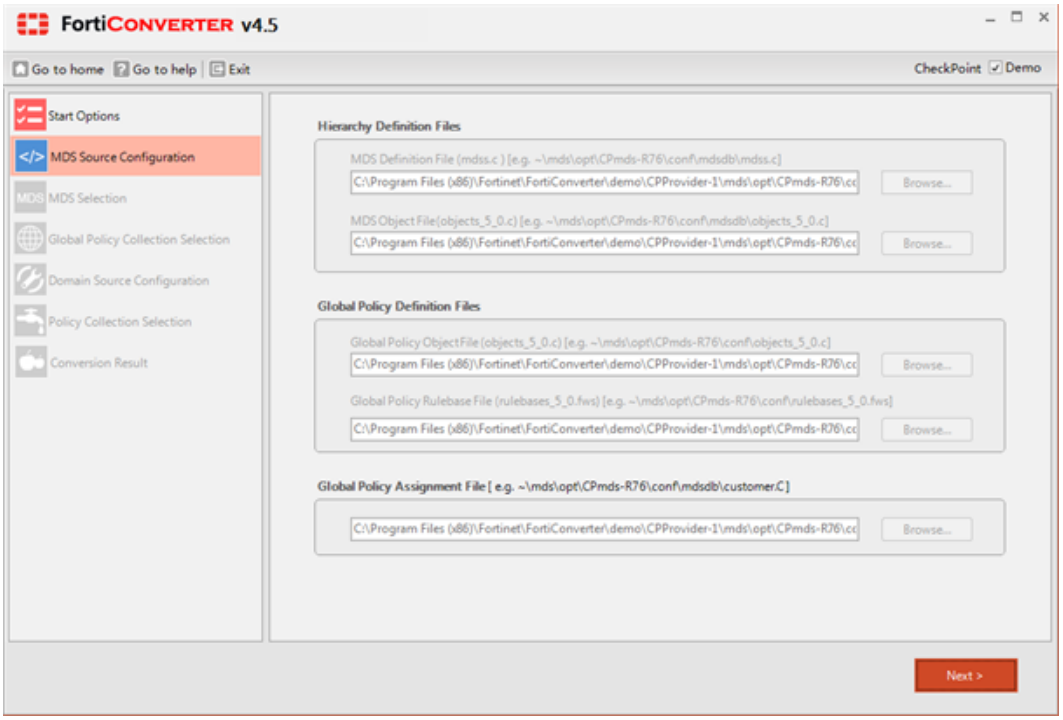
   For example, specify your old firewall or centralized management model, whether the output is for FortiGate or FortiManager, whether or not to discard unreferenced objects and comments, and the directory where you want to save output files.



You can also define how to handle the “Day in Month” setting on Check Point firewalls. Check Point firewalls have a time object that specifies days of the month,

which does not exist on FortiGate. By default, FortiConverter creates FortiGate one-time schedules for a year – one schedule per date. You can specify that FortiConverter creates more than one year of schedules, or select 0 to create no schedules. For more information, see the Check Point section in "Understanding your new configuration" on page 37.

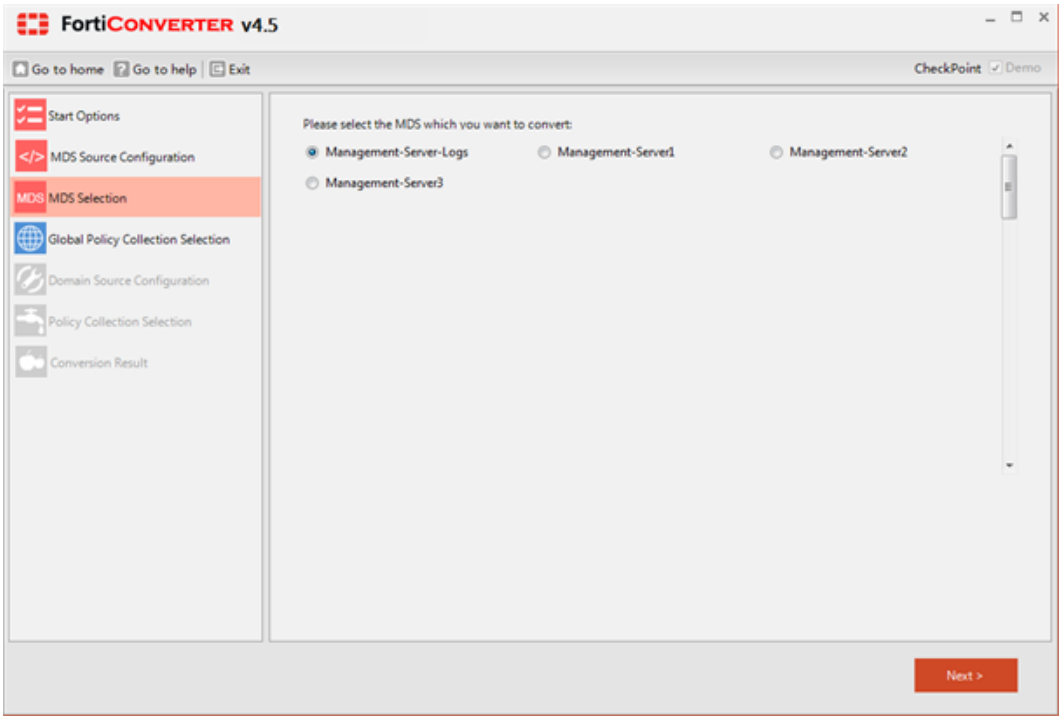
3. Click **Next**.
4. On the MDS Source Configuration page, browse to the configuration files that you obtained earlier to select them.



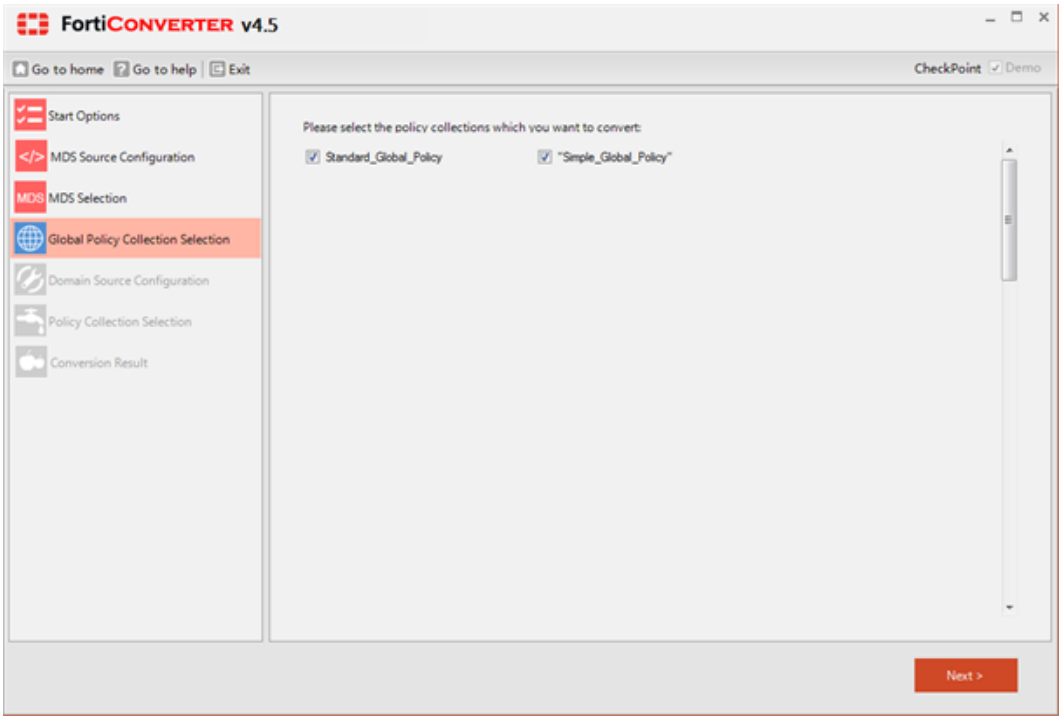
5. Click **Next**.

   Because MDS files can be very large, if the loading process takes more than a few seconds, a progress indicator is displayed.

6. Select which component in the MDS file to convert.

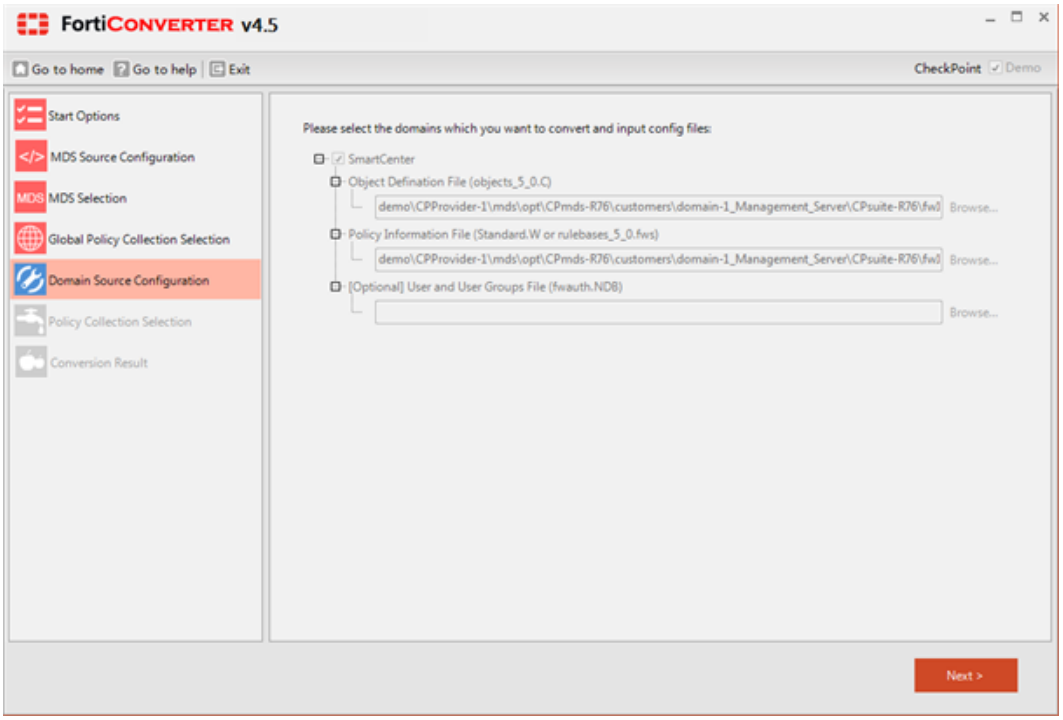


7. Click **Next**.
8. Select which collections of global policies to convert.



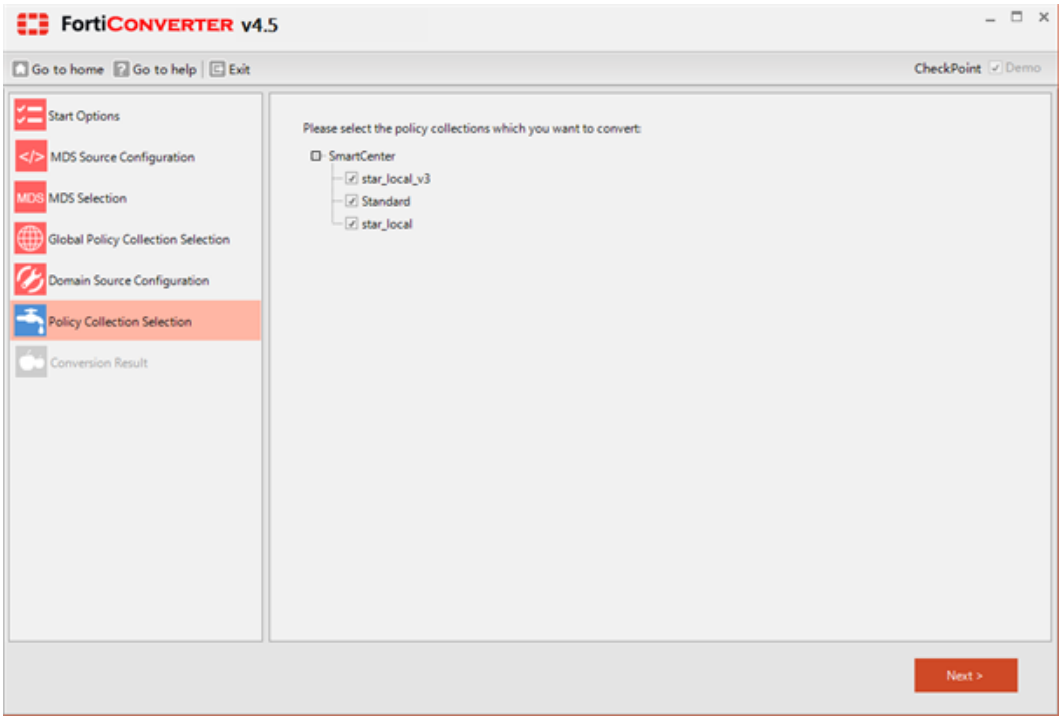
9. Click **Next**.

10. Select which domains to convert.

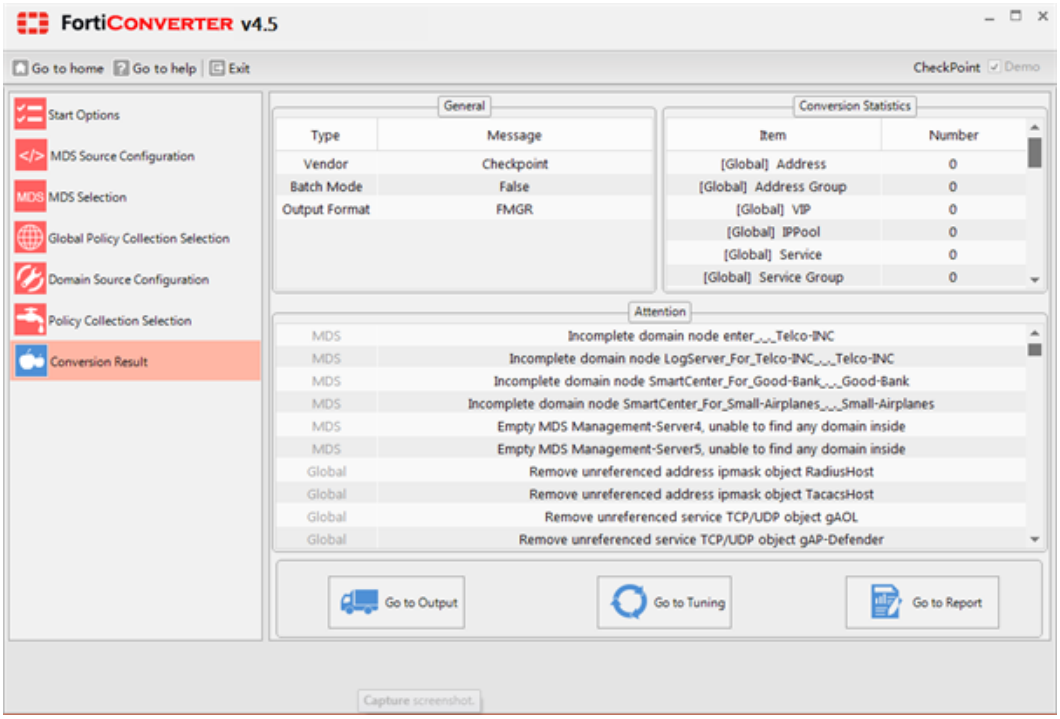


11. Click **Next**.

12. Select which policies to convert from the domains that you selected.



13. Click **Next**.



14. Do one of the following:

- Click **Go to Report** to see a summary of the conversion, including objects that the wizard did not convert. For more information, see "Viewing the results of your automatic conversion" on page 32.
- Click **Go to Tuning** to adjust the converted settings before you generate the final output configuration. For more informatinon, see "Fine-tuning" on page 33.
- Click **Go to Output** to view the final converted configuration files.

Using retail branch batch conversion mode

In the retail industry and other sectors, enterprises often deploy the same firewall configuration at a large number of remote sites. Instead of converting each site individually, the FortiConverter **Retail Branch Batch Mode** option allows you to use the wizard to convert all these sites in a single operation.

Typically, these firewall configurations have one or two network interfaces that connect to a WAN and differ only in the specified LAN and WAN IP addresses, the device name, and a few configuration objects.

Because the batch mode converts the specified group of configurations to a FortiGate configuration with a standard interface mapping, it requires that all the source configurations have the same number of network interfaces. The wizard applies the **FG Port** values that you

specify in the wizard's physical port mapping settings to all the output configurations. If any of the source configurations you select have a different number of interfaces, the wizard displays an alert.

Most of the conversion wizard steps are the same as when you convert a single configuration. However, the fine tuning feature you can use to edit the conversion configuration is not available in batch mode.

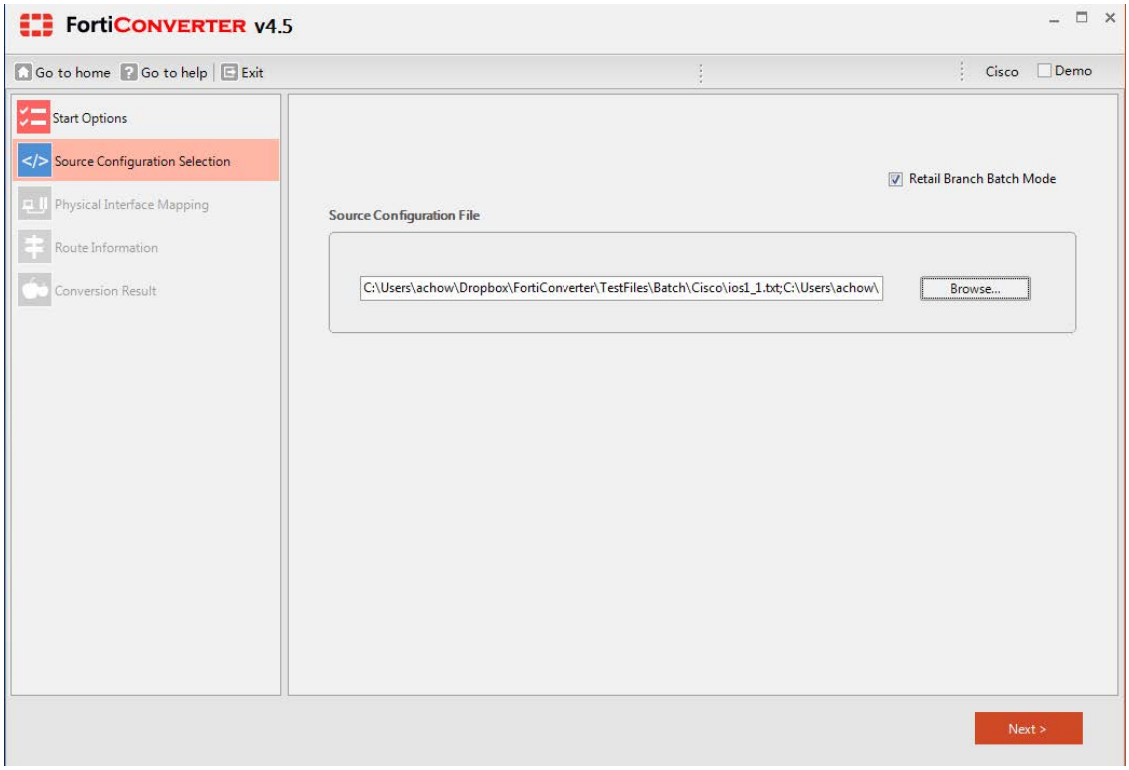
If any of your sites has a unique configuration or needs to be customized (for example, a firewall at the head office), do not use the **Retail Branch Batch Mode** option. Instead, see the instructions for converting a single configuration. (See "Using the conversion wizard" on page 17.)

Batch mode for Cisco, Juniper, Palo Alto Networks, and SonicWall firewalls

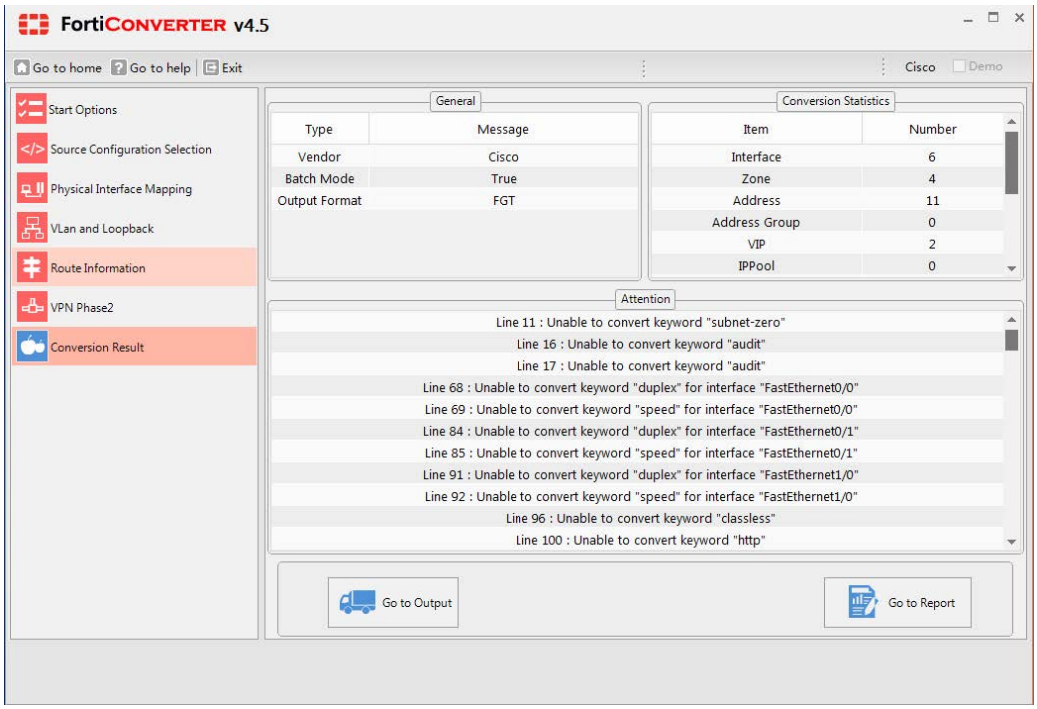
To enable batch mode when you convert Cisco, Juniper, Palo Alto Networks, and SonicWall firewalls, on the wizard's Source Configuration Selection page, select **Retail Branch Batch Mode**.

Click **Browse** to navigate to and select the configuration files. You can select multiple files.

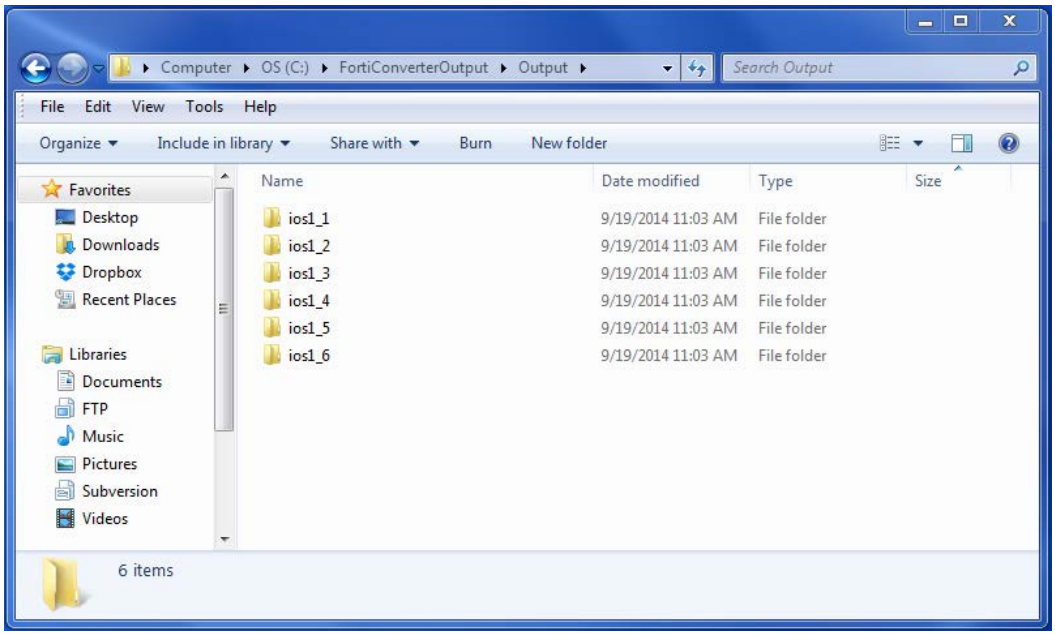
The wizard displays the selected files in a single line in the **Source Configuration File** field.



All other steps for using the wizard at the same as when you convert a single configuration, except for the **Conversion Result** page, which does not display the **Got to Tuning** option.



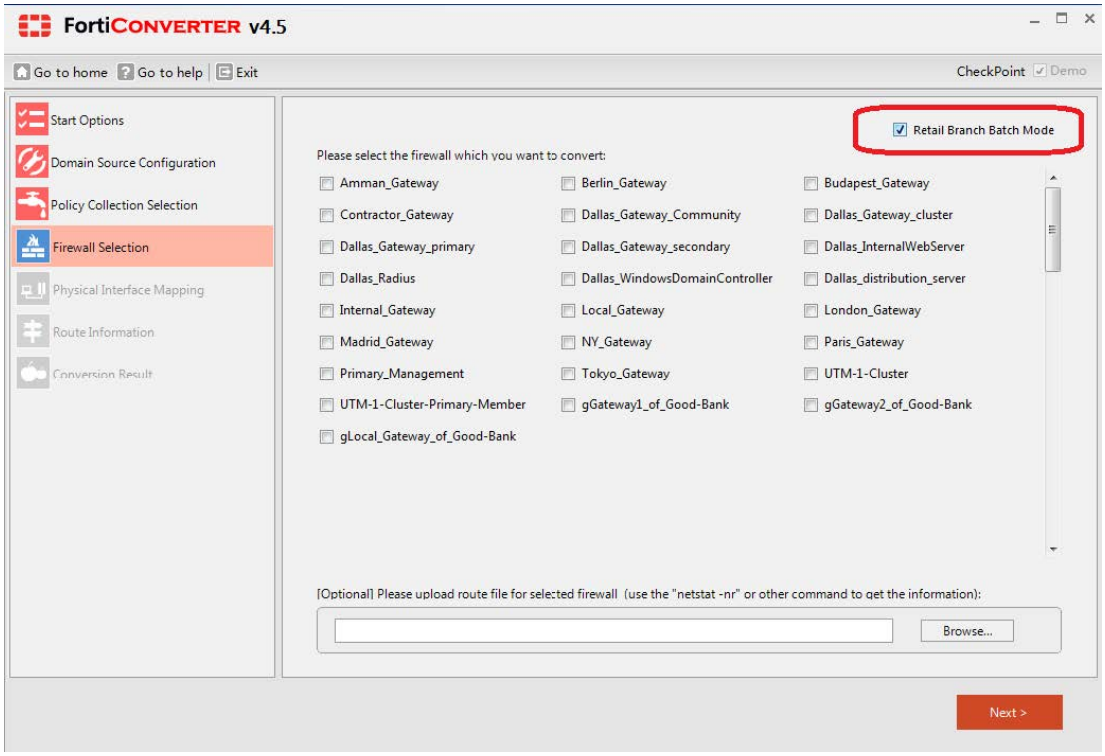
For batch conversion, the wizard saves each configuration file in its own directory in the output directory.



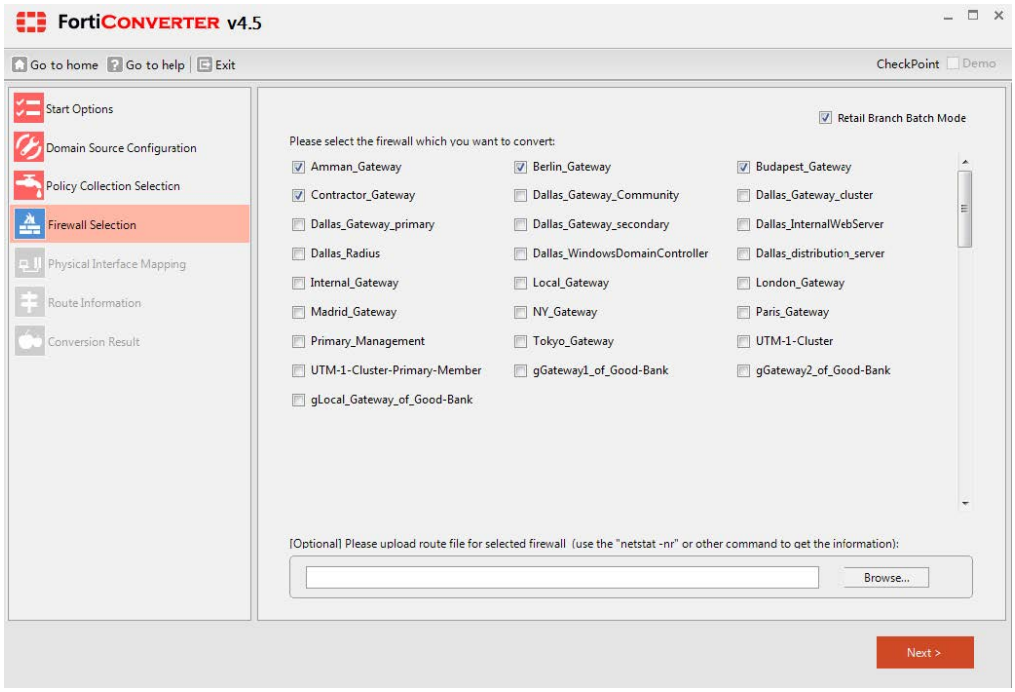
Batch mode for Alcatel-Lucent and Check Point firewalls

For Check Point and Alcatel-Lucent firewalls, batch mode can convert multiple firewalls within a configuration. You select the same input configuration and output settings as when

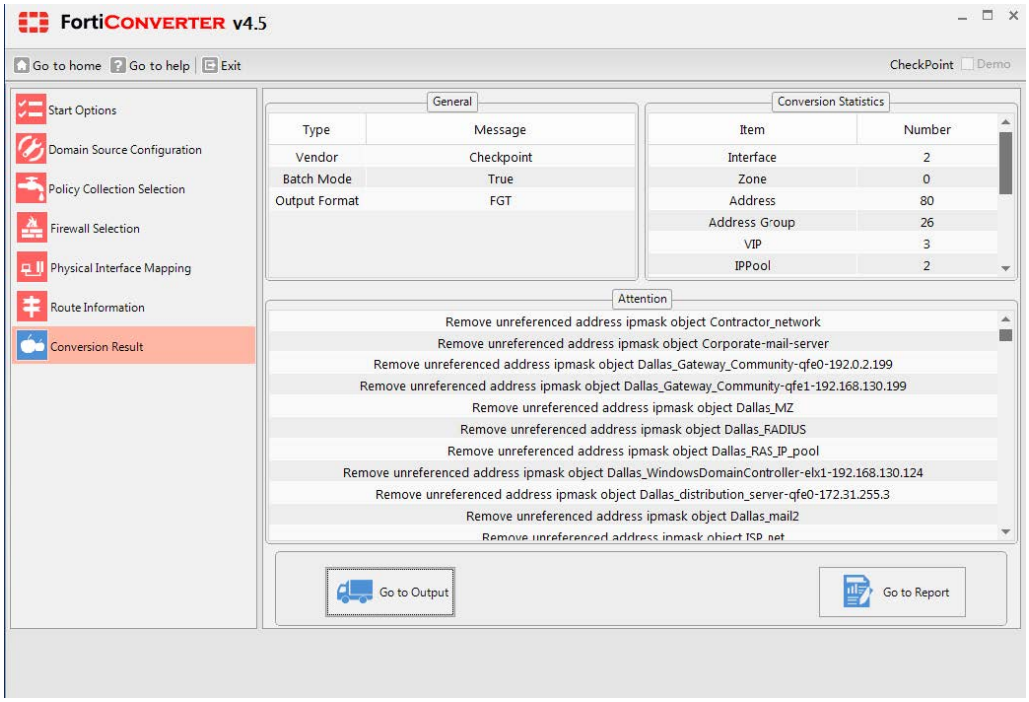
you convert a single configuration. Then, on the Firewall Selection page (Check Point) or Device Selection page (Alcatel-Lucent), select **Retail Branch Batch Mode**.



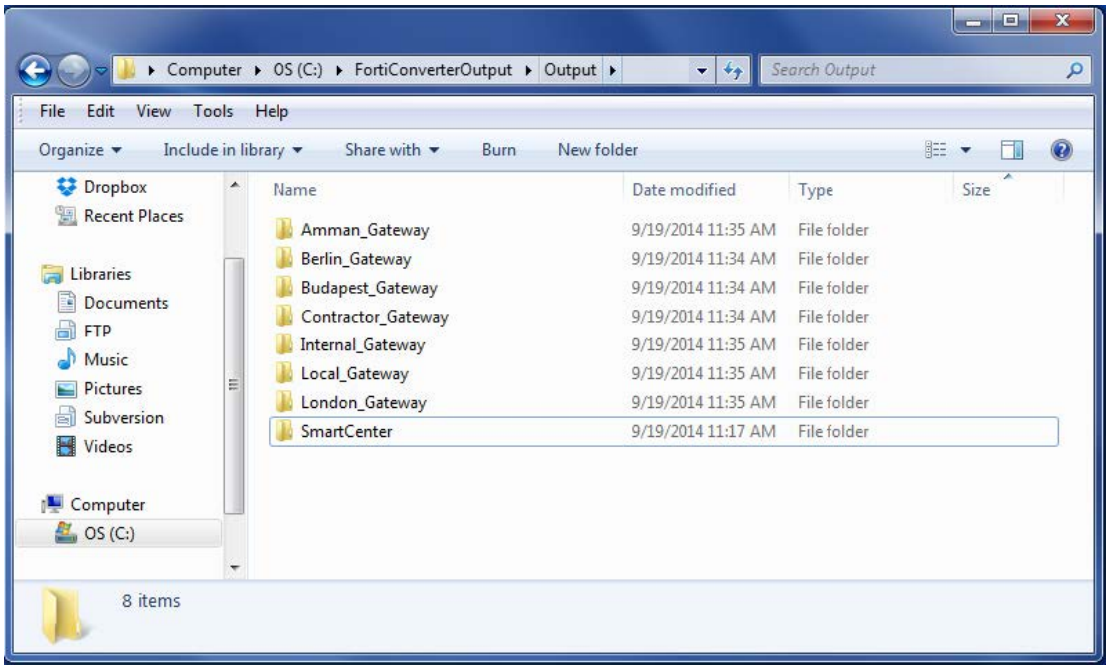
Select the firewalls to convert. Batch conversion requires that all the firewalls have the same number of network interfaces.



All other steps for using the wizard at the same as when you convert a single configuration, except for the **Conversion Result** page, which does not display the **Go to Tuning** option.



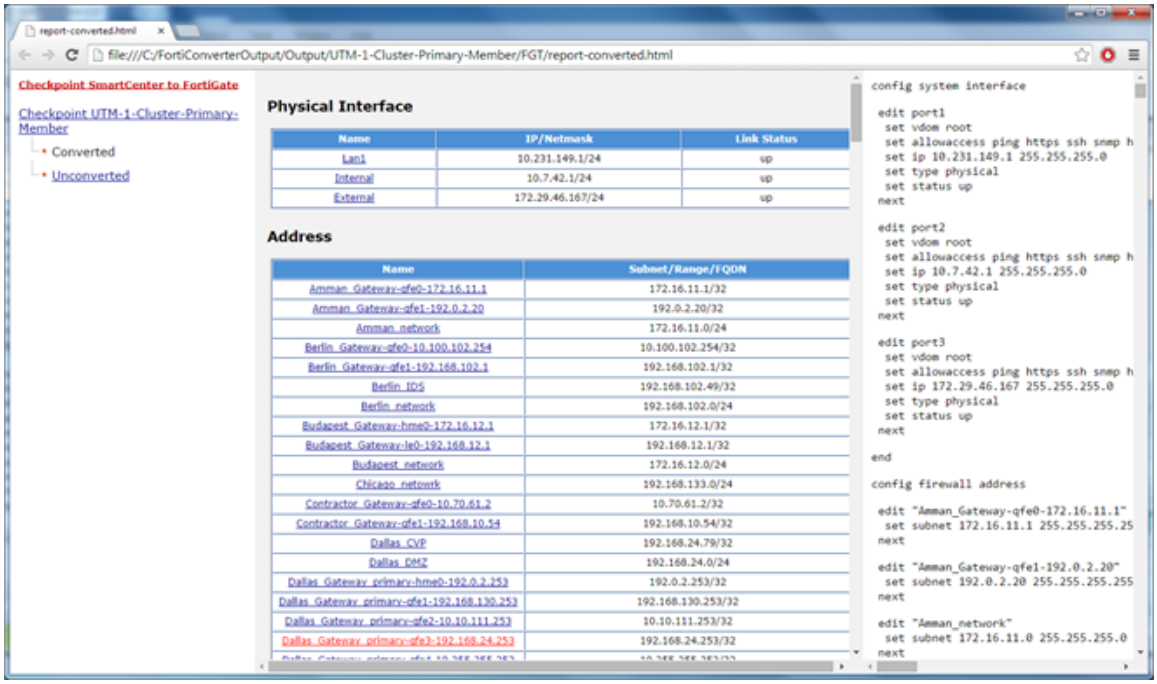
For batch conversions, the wizard saves each configuration file in its own directory in the output directory.



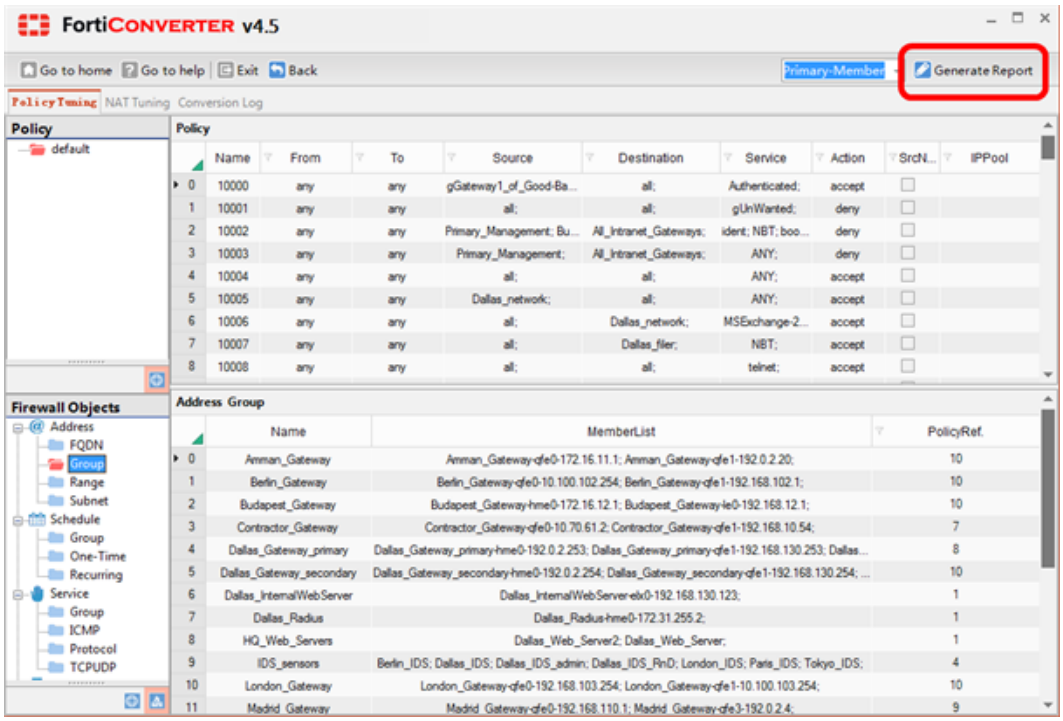
Viewing the results of your automatic conversion

To see a summary of the conversion, including objects that FortiConverter could not convert (and therefore require fine-tuning or manual conversion), on the Conversion Result page, click **Go to Report**.

FortiConverterdisplays the summary of the conversion in your web browser.



Alternatively, click **Go to Tuning**, make changes to the conversion configuration, and then click **Generate Report**.



FortiConverter regenerates the report based on the new settings.

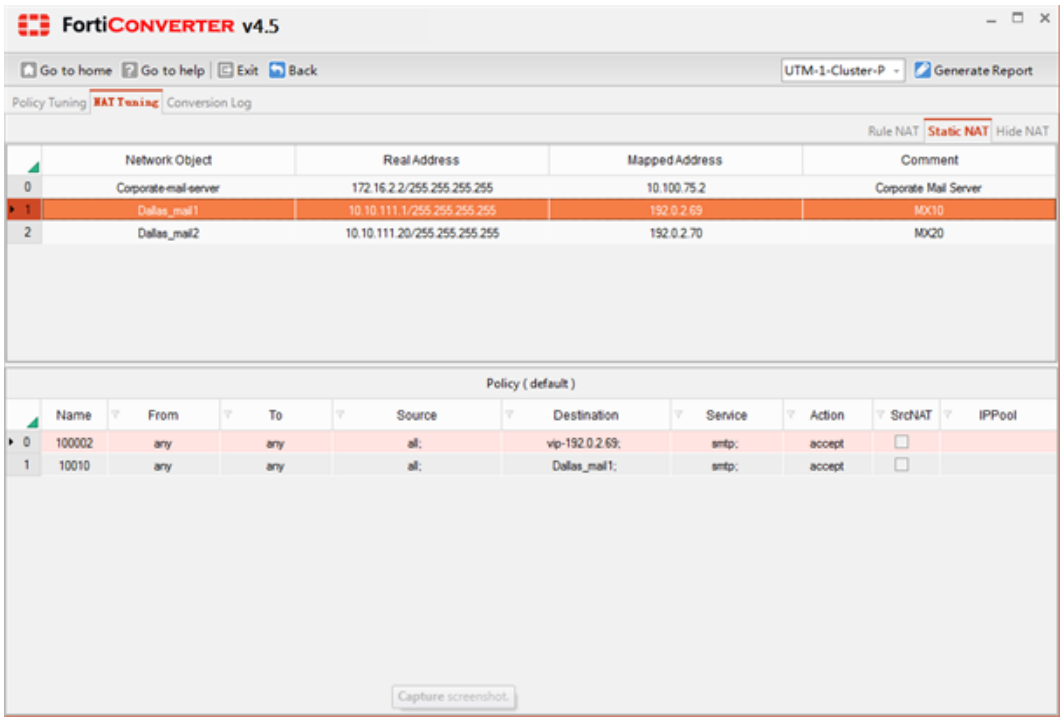
Fine-tuning

After FortiConverter has translated as many of your configuration objects as possible, you can fine-tune the result by adding objects that could not be converted or changing settings. To fine-tune the conversion, on the Conversion Result page, click **Go to Tuning**.

After your fine-tuning is complete, on the Conversion Result page, click **Go to Output** to access the final, converted configuration files.

Fine-tuning NAT conversion

FortiConverter divides NAT into one or more of the following categories: Source NAT, Destination NAT, Static NAT, Object NAT, Double NAT, and NAT Rule. The source configuration determines which categories are displayed.



FortiConverter automatically converts Juniper-ScreenOS configurations in which NAT is configured inside a policy. You do not need to fine-tune these types of configurations.

In cases where interfaces/addresses and service match completely, FortiConverter automatically merges NAT into the policy.

Polices with a number starting at 100000 are pure NAT policies. Merge these policies manually. Always place them at the bottom, below all security policies.

To add a new policy

1. Right click any row in the policy table, and then click **New**.
2. Enter the values for the new policy, and then click **OK**.

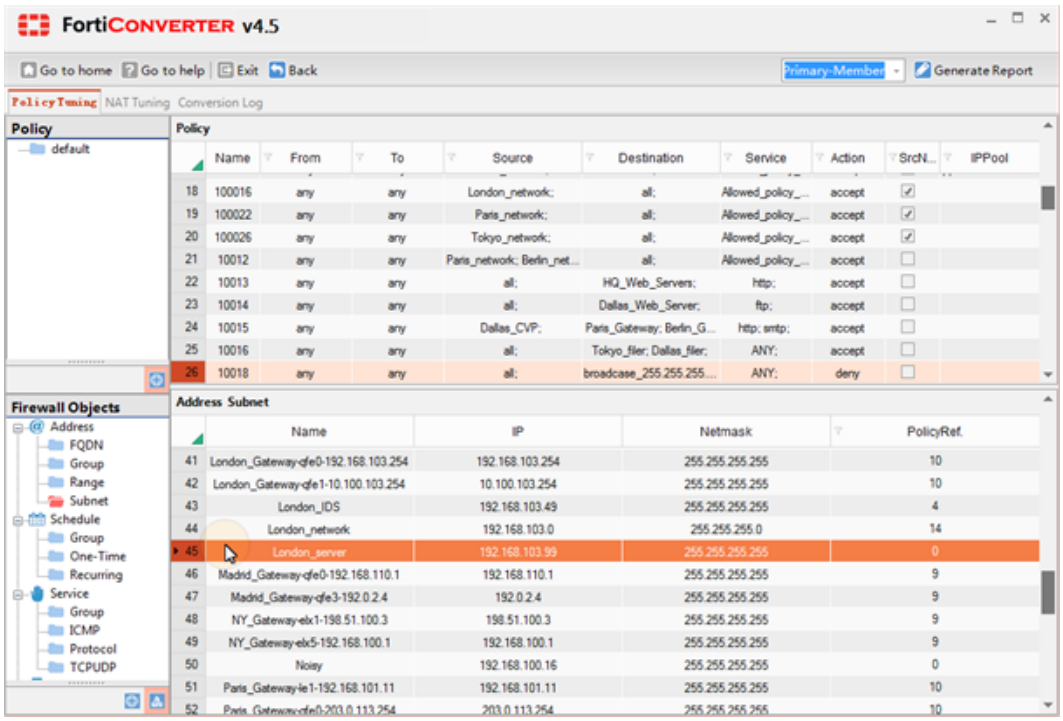
To renumber policies

1. Right click any row in the policy table, and then click **ConfigPolicyIndex**.
2. For **Set Policy Index Start With**, enter the initial policy number to use, and then click **OK**.

To delete a line of the configuration

Click the row's index number to select it, then press the **DELETE** key.

You cannot delete an items that are referenced by a policy or group.



Finding references to objects

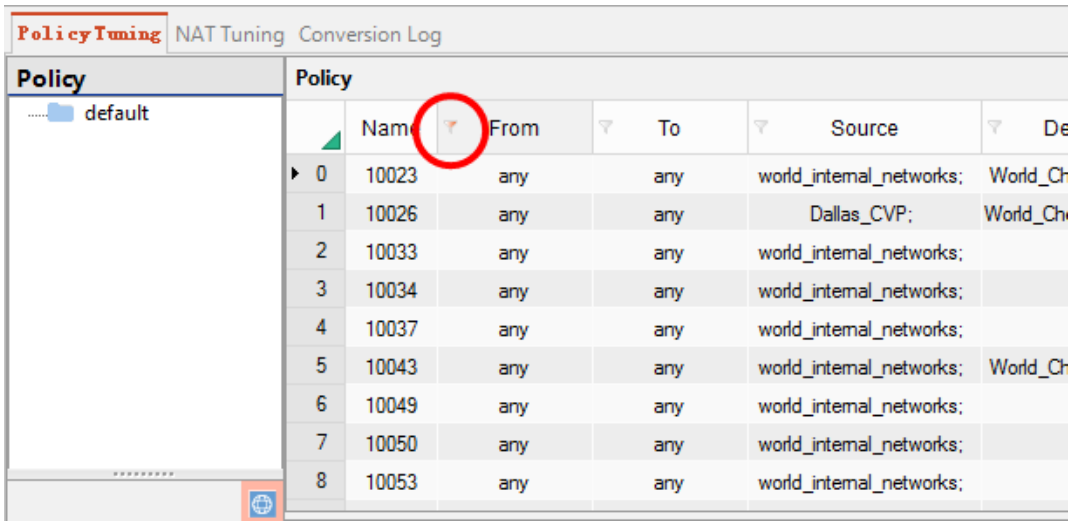
The PolicyRef. column displays the number of polices that reference that firewall object.

Click the PolicyRef. column for the Address Subnet entry to display the specific policies in the Policy table above.

You cannot delete objects that are referenced by any other part of the configuration.

Filtering rows to display only matching data

You can filter every column that has the [filter mark] by a given option or custom expression.



Reordering rows

To reorder rows, drag them into the new position.

Understanding your new configuration

To help you understand your new configuration, review the differences between FortiGate and FortiManager and your previous firewall.

Alcatel-Lucent differences

Conversion support

FortiConverter supports the conversion of the following Alcatel-Lucent Brick features:

- Interfaces
- Host Groups
- Service Groups
- Zone Brick Rulesets

Fortinet plans to support for the following Lucent features in a future FortiConverter release:

- NAT
- Schedule
- VPN
- Hosts Behind Zone

Address and address group configuration

- Lucent host addresses are mapped to FortiGate addresses.
- Lucent host groups are mapped to FortiGate address groups.
- Virtual Brick Addresses (VBA) are not supported.

Interface configuration

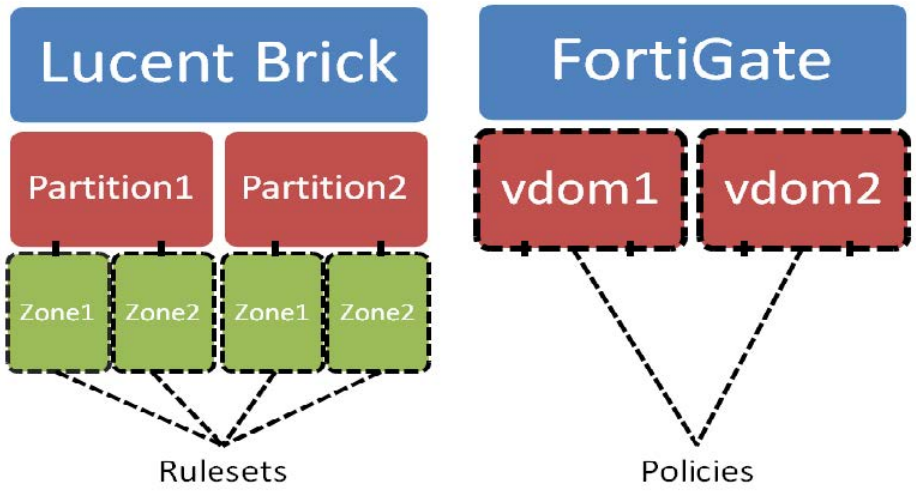
- FortiConverter assigns default VLAN configuration directly to physical interfaces.
- FortiConverter considers all VLANS named “*” or “Port Default”to be the default VALN configuration.
- Domain Addresses are not supported.

Service and Service Group configuration

- Lucent Service Groups are mapped to FortiGate Service Groups.
- Lucent service "*" maps to FortiGate service "any".

Policy configuration

Lucent Brick Zone Rulesets operate at the zone level, which has no direct equivalent in FortiGate. Zone rulesets need to be translated into equivalent FortiGate policies.



FortiConverter translates Lucent Brick rules by separating traffic into two categories: inter-partition and intra-partition.

- **Inter-partition traffic** behaves like inter-VDOM traffic, and is simple to convert to FortiGate policies.
- **Intra-partition traffic** is more complicated to convert because multiple zone rules can be applied.

FortiConverter handles the inter-partition traffic by creating a general policy for each rule.

FortiConverter handles the intra-partition traffic by looking for all matches between two zone rulesets. FortiConverter looks at 3 fields: source, destination, and service. All 3 fields must overlap for the rules to match. FortiConverter creates a policy for each match using the intersection of each field.

The action of the rules determines the action of the converted policy, as shown in the following table:

Rule 1	Rule 2	Policy
Pass	Pass	Accept
Pass	Drop	Deny

Rule 1	Rule 2	Policy
Drop	Pass	Deny
Drop	Drop	Deny

Inter-partition Deny policies have higher priority than intra-partition policies, while inter-partition Accept policies have lower priority than intra-partition policies.

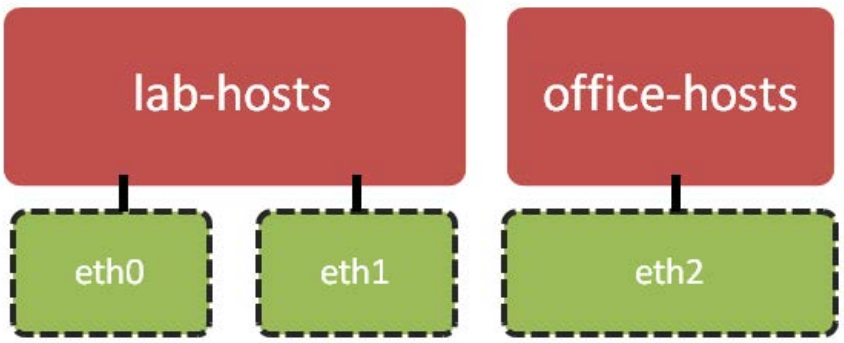
Lucent default rulesets “firewall” and “administrativezone” are currently unsupported.

VDOM configuration

- Lucent partitions map to FortiGate VDOMs.
- VDOM names are limited to 11 characters. FortiConverter truncates longer names to 11 characters.
- Lucent partition “*Default” maps to the FortiGate root VDOM.

Example conversion

The following block diagram and tables illustrates a Lucent configuration with 2 partitions and 3 zones.



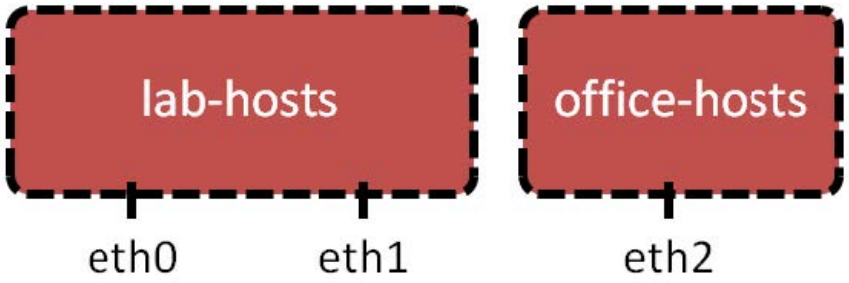
Zone eth0 Ruleset					
Rule Num	Direction	Source	Destination	Service	Action
1000	Out	192.168.1.15	172.30.10.1/24	*	Drop
1001	Both	192.168.1.0/24	172.30.10.1/24	*	Pass

Zone eth1 Ruleset					
Rule Num	Direction	Source	Destination	Service	Action
1000	In	*	172.30.10.5 - 172.30.10.20	TCP	Pass

Zone eth1 Ruleset					
Rule Num	Direction	Source	Destination	Service	Action
1001	Both	192.168.1.132	172.30.10.9	*	Pass

Zone eth2 Ruleset					
Rule Num	Direction	Source	Destination	Service	Action
1000	Both	*	10.10.15.0/24	HTTP	Pass

This Lucent configuration creates the following FortiGate configuration. Inter-partition rules are in **bold**.



VDOM lab-hosts Policies						
Policy Num	Src Inter-face	Dst Inter-face	Source	Destination	Service	Action
10000	**eth0**	**any**	**192.168.1.15**	**172.30.10.1/24**	*	**Deny**
10001	eth0	eth1	192.168.1.0/24	172.30.10.5 - 172.30.10.20	TCP	Accept
10002	eth0	eth1	192.168.1.132	172.30.10.9	*	Accept
10003	**eth0**	**any**	**192.168.1.0/24**	**172.30.10.1/24**	*	**Accept**
10004	any	eth0	192.168.1.0/24	172.30.10.1/24	*	Accept
10005	eth1	eth0	192.168.1.132	172.30.10.9	*	Accept
10006	**eth1**	**any**	**192.168.1.132**	**172.30.10.9**	*	**Accept**
10007	**any**	**eth1**	**192.168.1.132**	**172.30.10.9**	*	**Accept**

VDOM office-hosts Policies						
Policy Num	Src Inter-ace	Dst Inter-face	Source	Destination	Service	Action
10000	**any**	**eth2**	**any**	**10.10.15.0/24**	**HTTP**	**Accept**
10001	**eth2**	**any**	**10.10.15.0/24**	**any**	**TCP**	**Accept**

Check Point differences

General

- FortiGate's `set allowaccess` command for interfaces does not exist on Check Point. Because FortiGate requires this setting, FortiConverter by default enables all services for interfaces.
- The interface "Lead to Internet" is a default static route on FortiGate.

Schedule configuration

FortiConverter converts "Day in month" time schedules to FortiGate one-time schedules. It converts "Day in week" and "None" schedules to recurring schedules.

You assign a year range for the "Day in month" schedule. If the specified day does not exist for a certain month, FortiConverter does not generate the one-time schedule for that month.

For example, the Check Point firewall's "Day in month" time schedule has the following parameters for each year:

```
Month: Jan/March/Sept.
Day: 1, 5, 31
Start and end time: 0:00 to 10:00
```

If you select `1` for **Convert 'Day in Month' to 'One Time Schedule' for next x years** in the FortiConverter conversion wizard and the current year value for the PC running FortiConverter is 2013, the wizard generates the following output for FortiGate one-time schedules:

```
From 0:00 Jan/1/2013 To 10:00 Jan/1/2013
From 0:00 Jan/5/2013 To 10:00 Jan/5/2013
From 0:00 Jan/31/2013 To 10:00 Jan/31/2013
From 0:00 Match/1/2013 To 10:00 Match/1/2013
From 0:00 Match/5/2013 To 10:00 Match/5/2013
From 0:00 Match/31/2013 To 10:00 Match/31/2013
From 0:00 Sept./1/2013 To 10:00 Sept./1/2013
From 0:00 Sept./5/2013 To 10:00 Sept./5/2013
```

Notice that FortiConverter does not generate a Sept. 31 schedule.

NAT and policy configuration

- In Check Point, static NAT for Check Point is a 1-to-1 IP relationship. In the FortiGate NAT policy found in the converted configuration, source NAT with an IP pool is not a 1-to-1 relationship.
- FortiConverter converts rule actions with "Client Auth" to FortiGate user-identity policies with the “Accept” action.

VPN configuration

- Check Point does not configure VPN within a firewall rule. When FortiConverter converts the configuration to FortiGate, it generates several VPN policies from non-"Lead to Internet" interfaces to the "Lead to Internet" (default route) interface.
- After FortiConverter converts the VPN configuration, the VPN policy's destination interface refers to the "Lead to Internet" interface.

  If you changed the default route's egress interface, you may need to update the VPN/Policy configuration manually.

Cisco IOS, PIX or ASA differences

- FortiGate’s `set allowaccess` command for interfaces does not exist on Cisco firewalls. Because FortiGate requires this setting, FortiConverter by default enables all services for interfaces.
- Cisco `object-group` objects have two types of service definitions. Because FortiGate services have both a source and destination port, FortiConverter can only convert `service-object` items into FortiGate services. By default, it does not convert the other type of service object, defined by `port- object`. FortiConverter generates FortiGate service objects from a Cisco ACL's protocol and source/destination port.
- On Cisco IPSec VPNs, Phase 1 (ISAKMP) supports more than two types of authentication methods. FortiGate supports only two types: `pre-share` and `rsa-sig`. Therefore,you must assign methods for each VPN connection. The wizard converts Cisco EZVPN configuration to FortiGate VPN policies from the “Intranet” interface to the interface which was assigned by the `crypto map interface` command.
- FortiConverter does not support the following Cisco configuration elements:
  - ASA objects for NAT and double NAT
  - Wild card netmasks for `access-list` and `object- group` objects
  - EZVPN conversion

For example, FortiConverter does not support `crypto ipsec profile <profile-name>` and `crypto isakmp profile <profile-name>` .

Juniper ScreenOS or JunOS differences

- FortiConverter recognizes interface names starting with "vlan" as logical interfaces.

Palo Alto Networks OS (PAN-OS) differences

Conversion support

FortiConverter does not support the following features

- VPN
- IPv6 address ranges
- IPv6 address subnets (will be supported in a future release)
- UTM

Configuration notes

- PAN-OS handles NAT and firewall policies with two separate modules, while FortiGate handles NAT within its policy module. FortiConverter makes a best effort attempt to map NAT rules onto each policy during the conversion, but you should review the results for accuracy.
- FortiConverter converts PAN-OS weekly schedules to FortiGate weekday schedules that are stored in a schedule group.

SonicWALL differences

Special characters

FortiGate reserves '#' (hash sign), '(', and ')' (open and close curved brackets) as special characters. You cannot use them in the configuration unless an escape sequence precedes them. FortiConverter replaces these characters with the characters: '*' (star), '[' and ']' (open and close square brackets).

Examples:

- The address book “SNWL #1” becomes “SNWL *1”.
- The service book "Citrix TCP (Session Reliability)” becomes "Citrix TCP [Session Reliability]".

Address book configuration

- On FortiGate address objects do not support MAC addresses. Therefore, the wizard does not migrate SonicWall MAC addresses.
- FortiConverter generates two extra address book entries: “Any” and “_Address_Null”.
  - “Any” is added because it is a default address book in SonicWall.
  - FortiConverter generates “_Address_Null” because FortiGate address groups do not allow a group without any members. Only empty address groups can refer to “_Address_Null”.

Service book configuration

- FortiConverter does note migrate SonicWall service objects that are predefined on FortiGate. For example, HTTP port 80 and HTTPS port 443.

Schedule configuration

- A SonicWall schedule group can contain only one “one-time” schedule and multiple “recur” schedules. The “one-time” schedule is an implicit object that you can embed in the schedule group. Because FortiGate defines each schedule group explicity, FortiConverter automatically generates “one-time” schedules for the SonicWall implicit schedules.
- FortiGate time schedule configuration does not support “24:00” (equal to the next day’s 00:00). It uses "00:00" instead. When FortiConverter converts a SonicWall "recur" time schedule such as “M 00:00 to 24:00”, it sets the end time to “00:00”.

Local User and User Group

- Because FortiConverter cannot parse the local user’s password string, it sets all passwords to “123456”.
- Unlike FortiConverter, SonicWall allows you to nest user groups. For example, in SonicWall, usergroup1 can be a member of usergroup1. FortiConverter removes any nested configurations.

Route configuration

- FortiConverter does not convert the VPN configuration, including a Tunnel Interface VPN (route-based VPN).
- FortiConverter does not convert automatically generated routes like connected route and host route.

NAT configuration

Because FortiGate configures NAT rules within a policy module, FortiConverter generates one policy entry for each SonicWall NAT rule. If the NAT status is enabled, then FortiConverter also sets the policy status to enabled. Numbering for NAT-generated policies ID starts at 10001. Normal policy rules start at 0.

For source NAT, FortiConverter creates a new IP pool object for the FortiGate policy's source address.

For example, the SonicWall configuration has the following NAT policy:

Original source	Translated source	Original Destination	Translated Destination	Original Service	Tranlated Service
All Interface IP	X2 IP	Any	Original	Any	Original

To convert this configuration to a FortiGate configuration, FortiConverter create a new IP pool object "ippool_X2 IP". It uses the prefix "ippool_" for each auto-generated IP pool object.

For destination NAT, FortiConverter creates a new VIP object for the FortiGate policy's destination address.

For example, the SonicWall configuration has the following destination NAT rule:

Original source	Translated source	Original destination	Translated destination	Original service	Translated service
LAN Subnets	Original	WoW Static IP	X0 IP	SSLVPN	Original

To convert this configuration to a FortiGate configuration, FortiConverter creates a new IP pool object "vip_X0 IP". It uses the prefix "vip_" for each auto-generated VIP object.

If the destination NAT only translates the port number, then the translated destination address is the same as the original and the new VIP object refers to the translated service object's name.

FortiConverter cannot convert some SonicWall destination NAT rules. FortiGate VIP objects require strict 1-to-1 mapping between the original IP/port and the translated IP/port. SonicWall NAT rules do not have this limitation.

For example, the following SonicWall destination NAT rule has a 1-to-many mapping:

Original source	Translated source	Original destination	Translated destination	Original service	Translated service
test_1112_grp	test_11_gw	test_12_gw	test_1211_ grp	Echo	Original

This rule translates the destination address "test_12_gw" to an address group "test_1211_ grp". Because FortiGateVIPs cannot implement this conversion, FortiConverter ingores this rule.

The following SonicWall destination NAT has a many-to-many mapping:

Org Src	Tran Src	Org Dest	Tran Dest	Org Serv	Tran Serv
test_11_gw	test_12_gw	test_1112_grp	test_1211_grp	Echo	Original

This rule translates the destination address group “test_1112_grp” to another address group “test_1211_grp”. If the address groups have a different number of addresses, the FortiGate VIP object cannot implement the destination NAT correctly and FortiConverter ignores this rule.